Twin bent functions, strongly regular Cayley graphs, and Hurwitz-Radon theory

Paul C. Leopardi *

Revised: 9 October 2016

Abstract

The real monomial representations of Clifford algebras give rise to two sequences of bent functions. For each of these sequences, the corresponding Cayley graphs are strongly regular graphs, and the corresponding sequences of strongly regular graph parameters coincide. Even so, the corresponding graphs in the two sequences are not isomorphic, except in the first 3 cases. The proof of this non-isomorphism is a simple consequence of a theorem of Radon.

1 Introduction

Two recent papers [7, 8] describe and investigate two infinite sequences of bent functions and their Cayley graphs. The bent function σ_m on $\mathbb{Z}_2^{2m}$ is described in the first paper [7], on generalizations of Williamson's construction for Hadamard matrices. The bent function τ_m on $\mathbb{Z}_2^{2m}$ is described in the second paper [8], which investigates some of the properties of the two sequences of bent functions. In this second paper it is shown that the bent functions σ_m and τ_m both correspond to Hadamard difference sets with the same parameters

$$(v_m, k_m, \lambda_m, n_m) = (4^m, 2^{2m-1} - 2^{m-1}, 2^{2m-2} - 2^{m-1}, 2^{2m-2}),$$

and that their corresponding Cayley graphs are both strongly regular with the same parameters $(v_m, k_m, \lambda_m, \lambda_m)$.

The main result of the current paper is the following.

*Australian Government - Bureau of Meteorology. mailto:paul.leopardi@gmail.com

Theorem 1. *The Cayley graphs of the bent functions σ_m and τ_m are isomorphic only when $m = 1, 2,$ or 3.*

The remainder of the paper is organized as follows. Section 2 outlines some of the background of this investigation. Section 3 includes further definitions used in the subsequent sections. Section 4 proves the main result, and resolves the conjectures and the question raised by the previous papers. Section 5 puts these results in context, and suggests future research.

2 Background

A recent paper of the author [7] describes a generalization of Williamson's construction for Hadamard matrices [10] using the real monomial representation of the basis elements of the Clifford algebras $\mathbb{R}_{m,m}$.

Briefly, the general construction uses some

$$A_k \in \{-1, 0, 1\}^{n \times n}, \quad B_k \in \{-1, 1\}^{b \times b}, \quad k \in \{1, \ldots, n\},$$

where the A_k are *monomial* matrices, and constructs

$$H := \sum_{k=1}^{n} A_k \otimes B_k, \tag{H0}$$

such that

$$H \in \{-1, 1\}^{nb \times nb} \quad \text{and} \quad HH^T = nbI_{(nb)}, \tag{H1}$$

i.e. H is a Hadamard matrix of order nb. The paper [7] focuses on a special case of the construction, satisfying the conditions

$$\begin{gathered}
A_j * A_k = 0 \quad (j \neq k), \quad \sum_{k=1}^{n} A_k \in \{-1, 1\}^{n \times n}, \\
A_k A_k^T = I_{(n)}, \\
A_j A_k^T + \lambda_{j,k} A_k A_j^T = 0 \quad (j \neq k), \\
B_j B_k^T - \lambda_{j,k} B_k B_j^T = 0 \quad (j \neq k), \\
\lambda_{j,k} \in \{-1, 1\}, \\
\sum_{k=1}^{n} B_k B_k^T = nbI_{(b)},
\end{gathered} \tag{1}$$

where $*$ is the Hadamard matrix product.

In Section 3 of the paper [7], it is noted that the Clifford algebra $\mathbb{R}^{2^m \times 2^m}$ has a canonical basis consisting of 4^m real monomial matrices, corresponding to the basis of the algebra $\mathbb{R}_{m,m}$, with the following properties:

Pairs of basis matrices either commute or anticommute. Basis matrices are either symmetric or skew, and so the basis matrices A_j, A_k satisfy

$$A_k A_k^T = I_{(2^m)}, \quad A_j A_k^T + \lambda_{j,k} A_k A_j^T = 0 \quad (j \neq k), \quad \lambda_{j,k} \in \{-1, 1\}. \tag{2}$$

Additionally, for $n = 2^m$, we can choose a transversal of n canonical basis matrices that satisfies conditions (1) on the A matrices,

$$A_j * A_k = 0 \quad (j \neq k), \quad \sum_{k=1}^{n} A_k \in \{-1, 1\}^{n \times n}. \tag{3}$$

Section 3 also contains the definition of $\mathit{\Delta}_m$, the restricted amicability / anti-amicability graph of $\mathbb{R}_{m,m}$, and the subgraphs $\mathit{\Delta}_m[-1]$ and $\mathit{\Delta}_m[1]$, as well as the term "transversal graph". These definitions are repeated here since they are used in the conjectures and question below.

Definition 1. *[7, p. 225]*

Let $\mathit{\Delta}_m$ be the graph whose vertices are the $n^2 = 4^m$ positive signed basis matrices of the real representation of the Clifford algebra $\mathbb{R}_{m,m}$, with each edge having one of two labels, -1 or 1:

- *Matrices A_j and A_k are connected by an edge labelled by -1 ("red") if they have disjoint support and are anti-amicable, that is, $A_j A_k^{-1}$ is skew.*
- *Matrices A_j and A_k are connected by an edge labelled by 1 ("blue") if they have disjoint support and are amicable, that is, $A_j A_k^{-1}$ is symmetric.*
- *Otherwise there is no edge between A_j and A_k.*

The subgraph $\mathit{\Delta}_m[-1]$ consists of the vertices of $\mathit{\Delta}_m$ and all edges in $\mathit{\Delta}_m$ labelled by -1. Similarly, the subgraph $\mathit{\Delta}_m[1]$ contains all of the edges of $\mathit{\Delta}_m$ that are labelled by 1.

A *transversal graph* for the Clifford algebra $\mathbb{R}_{m,m}$ is any induced subgraph of $\mathit{\Delta}_m$ that is a complete graph on 2^m vertices. That is, each pair of vertices in the transversal graph represents a pair of matrices, A_j and A_k with disjoint support.

The following three conjectures appear in Section 3 of the paper [7]:

Conjecture 1. *For all $m \geqslant 0$ there is a permutation π of the set of 4^m canonical basis matrices, that sends an amicable pair of basis matrices with disjoint support to an anti-amicable pair, and vice-versa.*

Conjecture 2. *For all $m \geqslant 0$, for the Clifford algebra $\mathbb{R}_{m,m}$, the subset of transversal graphs that are not self-edge-colour complementary can be arranged into a set of pairs of graphs with each member of the pair being edge-colour complementary to the other member.*

Conjecture 3. *For all $m \geqslant 0$, for the Clifford algebra $\mathbb{R}_{m,m}$, if a graph T exists amongst the transversal graphs, then so does at least one graph with edge colours complementary to those of T.*

Note that Conjecture 1 implies Conjecture 2, which in turn implies Conjecture 3.

The significance of these conjectures can be seen in relation to the following result, which is Part 1 of Theorem 10 of the paper [7].

Lemma 1. *If b is a power of 2, $b = 2^m$, $m \geqslant 0$, the amicability / anti-amicability graph P_b of the matrices $\{-1, 1\}^{b \times b}$ contains a complete two-edge-coloured graph on $2b^2$ vertices with each vertex being a Hadamard matrix. This graph is isomorphic to $\mathit{\Gamma}_{m,m}$, the amicability / anti-amicability graph of the group $\mathbb{G}_{m,m}$.*

The definitions of $\mathit{\Gamma}_{m,m}$ and $\mathbb{G}_{m,m}$ are given in Section 3 of the paper [7], and the definition of $\mathbb{G}_{m,m}$ is repeated below. For the current paper, it suffices to note that $\mathit{\Delta}_m$ is a subgraph of $\mathit{\Gamma}_{m,m}$, and so, therefore, are all of the transversal graphs.

An n-tuple of A matrices of order $n = 2^m$ satisfying properties (2) and (3) yields a corresponding transversal graph T. As noted in Section 5 of the paper [7], if Conjecture 3 were true, this would guarantee the existence of an edge-colour complementary transversal graph $\overline{T}$. In turn, because Lemma 1 guarantees the existence of a complete two-edge-coloured graph isomorphic to $\mathit{\Gamma}_{m,m}$ within P_b, and because $\mathit{\Delta}_m$ is a subgraph of $\mathit{\Gamma}_{m,m}$, the graph P_b would have to contain a two-edge-coloured subgraph isomorphic to $\overline{T}$. This would imply the existence of an n-tuple of B matrices of order n satisfying the condition (1) such that the construction (H0) would satisfy the Hadamard condition (H1), with a matrix of order n^2.

The author's subsequent paper on bent functions [8] refines Conjecture 1 into the following question.

Question 1. *Consider the sequence of edge-coloured graphs $\mathit{\Delta}_m$ for $m \geqslant 1$, each with red subgraph $\mathit{\Delta}_m[-1]$, and blue subgraph $\mathit{\Delta}_m[1]$. For which $m \geqslant 1$ is there an automorphism of $\mathit{\Delta}_m$ that swaps the subgraphs $\mathit{\Delta}_m[-1]$ and $\mathit{\Delta}_m[1]$?*

The main result of this paper, Theorem 1, leads to the resolution of these conjectures and this question.

3 Further definitions and properties

This section sets out the remainder of the definitions and properties used in this paper. It is based on the previous papers [7, 8] with additions.

Clifford algebras and their real monomial representations. The following definitions and results appear in the paper on Hadamard matrices and Clifford algebras [7], and are presented here for completeness, since they are used below. Further details and proofs can be found in that paper, and in the paper on bent functions [8], unless otherwise noted. An earlier paper on representations of Clifford algebras [6] contains more background material.

The signed group [2] $\mathbb{G}_{p,q}$ of order 2^{1+p+q} is extension of $\mathbb{Z}_2$ by $\mathbb{Z}_2^{p+q}$, defined by the signed group presentation

$$\begin{aligned}\mathbb{G}_{p,q} := \Big\langle\ & \mathbf{e}_{\{k\}}\ (k \in S_{p,q}) \ \mid \\ & \mathbf{e}_{\{k\}}^2 = -1\ (k < 0), \quad \mathbf{e}_{\{k\}}^2 = 1\ (k > 0), \\ & \mathbf{e}_{\{j\}}\mathbf{e}_{\{k\}} = -\mathbf{e}_{\{k\}}\mathbf{e}_{\{j\}}\ (j \neq k) \Big\rangle,\end{aligned}$$

where $S_{p,q} := \{-q, \ldots, -1, 1, \ldots, p\}$.

The 2×2 orthogonal matrices

$$\mathrm{E}_1 := \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \quad \mathrm{E}_2 := \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

generate $P(\mathbb{G}_{1,1})$, the real monomial representation of group $\mathbb{G}_{1,1}$. The cosets of $\{\pm I\} \equiv \mathbb{Z}_2$ in $P(\mathbb{G}_{1,1})$ are ordered using a pair of bits, as follows.

$$\begin{aligned} 0 &\leftrightarrow 00 \leftrightarrow \{\pm I\}, \\ 1 &\leftrightarrow 01 \leftrightarrow \{\pm \mathrm{E}_1\}, \\ 2 &\leftrightarrow 10 \leftrightarrow \{\pm \mathrm{E}_2\}, \\ 3 &\leftrightarrow 11 \leftrightarrow \{\pm \mathrm{E}_1\mathrm{E}_2\}. \end{aligned}$$

For $m > 1$, the real monomial representation $P(\mathbb{G}_{m,m})$ of the group $\mathbb{G}_{m,m}$ consists of matrices of the form $G_1 \otimes G_{m-1}$ with G_1 in $P(\mathbb{G}_{1,1})$ and G_{m-1}

in $P(\mathbb{G}_{m-1,m-1})$. The cosets of $\{\pm I\} \equiv \mathbb{Z}_2$ in $P(\mathbb{G}_{m,m})$ are ordered by concatenation of pairs of bits, where each pair of bits uses the ordering as per $P(\mathbb{G}_{1,1})$, and the pairs are ordered as follows.

$$\begin{aligned}
0 &\leftrightarrow 00\ldots00 \leftrightarrow \{\pm I\},\\
1 &\leftrightarrow 00\ldots01 \leftrightarrow \{\pm I_{(2)}^{\otimes(m-1)} \otimes \mathrm{E}_1\},\\
2 &\leftrightarrow 00\ldots10 \leftrightarrow \{\pm I_{(2)}^{\otimes(m-1)} \otimes \mathrm{E}_2\},\\
&\ldots\\
2^{2m}-1 &\leftrightarrow 11\ldots11 \leftrightarrow \{\pm(\mathrm{E}_1\mathrm{E}_2)^{\otimes m}\}.
\end{aligned}$$

This ordering is called the *Kronecker product ordering* of the cosets of $\{\pm I\}$ in $P(\mathbb{G}_{m,m})$.

The group $\mathbb{G}_{m,m}$ and its real monomial representation $P(\mathbb{G}_{m,m})$ satisfy the following properties.

1. Pairs of elements of $\mathbb{G}_{m,m}$ (and therefore $P(\mathbb{G}_{m,m})$) either commute or anticommute: for $g, h \in \mathbb{G}_{m,m}$, either $hg = gh$ or $hg = -gh$.
2. The matrices $E \in P(\mathbb{G}_{m,m})$ are orthogonal: $EE^T = E^TE = I$.
3. The matrices $E \in P(\mathbb{G}_{m,m})$ are either symmetric and square to give I or skew and square to give $-I$: either $E^T = E$ and $E^2 = I$ or $E^T = -E$ and $E^2 = -I$.

Taking the positive signed element of each of the 2^{2m} cosets listed above defines a transversal of $\{\pm I\}$ in $P(\mathbb{G}_{m,m})$ which is also a monomial basis for the real representation of the Clifford algebra $\mathbb{R}_{m,m}$ in Kronecker product order, called this basis the *positive signed basis* of $P(\mathbb{R}_{m,m})$.

The function $\gamma_m : \mathbb{Z}_{2^{2m}} \to P(\mathbb{G}_{m,m})$ chooses the corresponding basis matrix from the positive signed basis of $P(\mathbb{R}_{m,m})$, using the Kronecker product ordering. This ordering also defines a corresponding function on $\mathbb{Z}_2^{2m}$, also called γ_m.

Hurwitz-Radon theory. The key concept used in the proof of Lemma 3 below is that of a *Hurwitz-Radon family* of matrices.

A set of real orthogonal matrices $\{A_1, A_2, \ldots, A_s\}$ is called a Hurwitz-Radon family [3, 4, 9] if

1. $A_j^T = -A_j$ for all $j = 1, \ldots, s$, and
2. $A_jA_k = -A_kA_j$ for all $j \neq k$.

The Hurwitz-Radon function ρ is defined by

$$\rho(2^{4d+c}) := 2^c + 8d, \quad \text{where } 0 \leqslant c < 4.$$

As stated by Geramita and Pullman [3], Radon [9] proved the following result, which is used as a lemma in this paper.

Lemma 2. *[3, Theorem A]*
Any Hurwitz-Radon family of order n has at most $\rho(n) - 1$ members.

The two sequences of bent functions.
The previous two papers [7, 8] define two binary functions on $\mathbb{Z}_2^{2m}$, σ_m and τ_m, respectively. Their key properties are repeated below. See the two papers for the proofs and for more details and references on bent functions.
The function $\sigma_m : \mathbb{Z}_2^{2m} \to \mathbb{Z}_2$ has the following properties.

1. For $i \in \mathbb{Z}_2^{2m}$, $\sigma_m(i) = 1$ if and only if the number of digits equal to 1 in the base 4 representation of i is odd.

2. Since each matrix $\gamma_m(i)$ is orthogonal, $\sigma_m(i) = 1$ if and only if the matrix $\gamma_m(i)$ is skew.

3. The function σ_m is bent.

The function $\tau_m : \mathbb{Z}_2^{2m} \to \mathbb{Z}_2$ has the following properties.

1. For $i \in \mathbb{Z}_2^{2m}$, $\tau_m(i) = 1$ if and only if the number of digits equal to 1 or 2 in the base 4 representation of i is non zero, and the number of digits equal to 1 is even.

2. The value $\tau_m(i) = 1$ if and only if the matrix $\gamma_m(i)$ is symmetric but not diagonal.

3. The function τ_m is bent.

The relevant graphs.
For a binary function $f : \mathbb{Z}_2^{2m} \to \mathbb{Z}_2$, with $f(0) = 0$ we consider the simple undirected *Cayley graph* $\mathrm{Cay}(f)$ [1, 3.1] where the vertex set $V(\mathrm{Cay}(f)) = \mathbb{Z}_2^{2m}$ and for $i, j \in \mathbb{Z}_2^{2m}$, the edge (i, j) is in the edge set $E(\mathrm{Cay}(f))$ if and only if $f(i + j) = 1$.
In the paper on Hadamard matrices [7] it is shown that since $\sigma_m(i) = 1$ if and only if $\gamma_m(i)$ is skew, the subgraph $\varDelta_m[-1]$ is isomorphic to the Cayley graph $\mathrm{Cay}(\sigma_m)$.

The paper on bent functions [8] notes that since $\tau_m(i) = 1$ if and only if $\gamma_m(i)$ is symmetric but not diagonal, the subgraph $\Delta_m[1]$ is isomorphic to the Cayley graph $\mathrm{Cay}(\tau_m)$. In that paper, these isomorphisms and the characterization of $\mathrm{Cay}(\sigma_m)$ and $\mathrm{Cay}(\tau_m)$ as Cayley graphs of bent functions are used to prove the following theorem.

Theorem 2. *[8, Theorem 5.2]*
For all $m \geqslant 1$, both graphs $\Delta_m[-1]$ and $\Delta_m[1]$ are strongly regular, with parameters $v_m = 4^m$, $k_m = 2^{2m-1} - 2^{m-1}$, $\lambda_m = \mu_m = 2^{2m-2} - 2^{m-1}$.

4 Proof of Theorem 1 and related results

Here we prove the main result, and examine its implications for Conjectures 1 to 3 and Question 1.

The proof of Theorem 1 follows from the following two lemmas. The first lemma puts an upper bound on the clique number of the graph $\mathrm{Cay}(\sigma_m) \simeq \Delta_m[-1]$.

Lemma 3. *The clique number of the graph $\mathrm{Cay}(\sigma_m)$ is at most $\rho(2^m)$, where ρ is the Hurwitz-Radon function. Therefore $\rho(2^m) < 2^m$ for $m \geqslant 4$.*

Proof. If we label the vertices of the graph $\mathrm{Cay}(\sigma_m)$ with the elements of Z_2^{2m}, then any clique in this graph is mapped to another clique if a constant is added to all of the vertices. Thus without loss of generality we can assume that we have a clique of order $s+1$ with one of the vertices labelled by 0. If we then use γ_m to label the vertices with elements of $\mathbb{R}_{m,m}$ to obtain the isomorphic graph $\Delta_m[-1]$, we have one vertex of the clique labelled with the identity matrix I of order 2^m. Since the clique is in $\Delta_m[-1]$, the other vertices A_1 to A_s (say) must necessarily be skew matrices that are pairwise anti-amicable,

$$A_j A_k^T = -A_k A_j^T \quad \text{for all } j \neq k.$$

But then

$$A_j A_k = -A_k A_j \quad \text{for all } j \neq k,$$

and therefore $\{A_1, \ldots, A_s\}$ is a Hurwitz-Radon family. By Lemma 2, s is at most $\rho(2^m) - 1$ and therefore the size of the clique is at most $\rho(2^m)$. □

The second lemma puts a lower bound on the clique number of the graph $\mathrm{Cay}(\tau_m) \simeq \Delta_m[1]$.

Lemma 4. *The clique number of the graph* $\mathrm{Cay}(\tau_m)$ *is at least* 2^m.

Proof. We construct a clique of order 2^m in $\mathrm{Cay}(\tau_m)$ with the vertices labelled in $\mathbb{Z}_2^{2m}$, using the following vertices denoted in base 4:

$$
\begin{gathered}
00\ldots02 \\
00\ldots20 \\
\ldots \\
22\ldots22
\end{gathered}
$$

This set is closed under addition in $\mathbb{Z}_2^{2m}$, and therefore forms a clique of order 2^m in $\mathrm{Cay}(\tau_m)$. ☐

With these two lemmas in hand, the proof of Theorem 1 follows easily.
Proof of Theorem 1. The result is a direct consequence of Lemmas 3 and 4. For $m \geqslant 4$, the clique numbers of the graphs $\mathrm{Cay}(\sigma_m)$ and $\mathrm{Cay}(\tau_m)$ are different, and therefore these graphs cannot be isomorphic. ☐

Lemmas 3 and 4, along with Theorem 1 imply the failure of the conjectures 1 to 3, as well as the resolution of Question 1, as follows.

Theorem 3. *For* $m \geqslant 4$ *the following hold.*

1. *There exist transversal graphs that do not have an edge-colour complement, and therefore Conjecture 3 does not hold.*

2. *As a consequence, Conjectures 1 and 2 also do not hold.*

3. *Question 1 is resolved. The only* $m \geqslant 1$ *for which there is an automorphism of* Δ_m *that swaps the subgraphs* $\Delta_m[-1]$ *and* $\Delta_m[1]$ *are* $m = 1, 2$ *and* 3.

Proof. Assume that $m \geqslant 4$. A transversal graph is a subgraph of Δ_m which is a complete graph of order 2^m. The edges of a transversal graph are labelled with the colour red (if the edge is contained in $\Delta_m[-1]$) or blue (if the edge is contained in $\Delta_m[1]$). By Lemma 3, the largest clique of $\Delta_m[-1]$ is of order $\rho(2^m) < 2^m$, and by Lemma 4, the largest clique of $\Delta_m[1]$ is of order 2^m. If we take a blue clique of order 2^m as a transversal graph, this cannot have an edge-colour complement in Δ_m, because no red clique can be this large. More generally, we need only take a transversal graph containing a blue clique with order larger than $\rho(2^m)$ to have a clique with no edge-colour complement in Δ_m. This falsifies Conjecture 3.

Since Conjecture 3 fails for $m \geqslant 4$, the pairing of graphs described in Conjecture 2 is impossible for $m \geqslant 4$. Thus Conjecture 2 is also false.

Finally, Conjecture 1 fails as a direct consequence of Theorem 1 since, for $m \geqslant 4$, the subgraphs $\varDelta_m[-1]$ and $\varDelta_m[1]$are not isomorphic. Therefore, for $m \geqslant 4$, there can be no automorphism of $\varDelta_m$ that swaps these subgraphs. □

5 Discussion

The result of Lemma 3 is well known. For example, the graph $\varDelta_m[-1]$ is the complement of the graph V^+ of Yiu [11], and the result for V^+ in his Theorem 2 is equivalent to Lemma 3.

The main consequence of Theorem 3 is that for $m > 3$ there is at least one n-tuple of A matrices, with $n = 2^m$ such that no n-tuple of B matrices of order n can be found to satisfy construction (H0) under condition (H1). The proof of Theorem 5 of the Hadamard construction paper [7] shows by construction that for any m, and any n-tuple of A matrices satisfying (1), there is an n-tuple of B matrices of order nc that satisfies construction (H0) under condition (H1), where $c = M(n-1)$, with

$$M(q) := \begin{cases} \lceil \frac{q}{2} \rceil + 1, & \text{if } q \equiv 2, 3, 4 \pmod 8, \\ \lceil \frac{q}{2} \rceil & \text{otherwise.} \end{cases} \tag{4}$$

Thus Theorem 5 remains valid. The question remains as to whether the the order nc is tight or can be reduced. In the special case where the n-tuple of A matrices is mutually amicable, the answer is given by Corollary 15 of the paper [7]: The set of $\{-1, 1\}$ matrices of order c contains an n-tuple of mutually anti-amicable Hadamard matrices. So in this special case, the required order can be reduced from nc to c. This leads to the following question.

Question 2. *In the general case, for any $m > 1$, $n = 2^m$, for any n-tuple of A matrices satisfying (1), does there always exist an n-tuple of B matrices of order c that satisfies construction (H0) under condition (H1), where $c = M(n-1)$, with M defined by (4)?*

As a result of Theorems 2 and 3, we see that we have two sequences of strongly regular graphs, $\varDelta_m[-1]$ and $\varDelta_m[1]$ $(m \geqslant 1)$, sharing the same parameters, $v_m = 4^m$, $k_m = 2^{2m-1} - 2^{m-1}$, $\lambda_m = \mu_m = 2^{2m-2} - 2^{m-1}$, but the graphs are isomorphic only for $m = 1, 2, 3$. For these three values of m, the existence of automorphisms of $\varDelta_m$ that swap $\varDelta_m[-1]$ and $\varDelta_m[1]$ as subgraphs [7, Table 1] is remarkable in the light of Theorem 3.

A paper of Bernasconi and Codenotti describes the relationship between bent functions and their Cayley graphs, implying that a bent function corresponding to a (v, k, λ, n) Hadamard difference set has a Cayley graph that

is strongly regular with parameters (v, k, λ, μ) where $\lambda = \mu$ [1, Lemma 12]. The current paper notes that for two specific sequences of bent functions, σ_m and τ_m, the corresponding Cayley graphs are not necessarily isomorphic.

This raises the subject of classifying bent functions via their Cayley graphs, raising the following questions.

Question 3. *Which strongly regular graphs with parameters (v, k, λ, λ) occur as Cayley graphs of bent functions?*

Question 4. *What is the relationship between other classifications of bent functions and the classification via Cayley graphs?*

This classification is the topic of a paper in preparation [5].

Acknowledgements. Thanks to Christine Leopardi for her hospitality at Long Beach. Thanks to Robert Craigen, Joanne Hall, William Martin, Padraig Ó Catháin and Judy-anne Osborn for valuable discussions. This work was begun in 2014 while the author was a Visiting Fellow at the Australian National University, continued while the author was a Visiting Fellow and a Casual Academic at the University of Newcastle, Australia, and concluded while the author was an employee of the Bureau of Meteorology of the Australian Government. Thanks also to the anonymous reviewers of previous drafts of this paper.

References

[1] A. Bernasconi and B. Codenotti. Spectral analysis of Boolean functions as a graph eigenvalue problem. *IEEE Transactions on Computers*, 48(3):345–351, (1999).

[2] R. Craigen. Signed groups, sequences, and the asymptotic existence of Hadamard matrices. *J. Combin. Theory Ser. A*, 71(2):241–254, (1995).

[3] A. V. Geramita and N. J. Pullman. A theorem of Hurwitz and Radon and orthogonal projective modules. *Proceedings of the American Mathematical Society*, 42(1):51–56, (1974).

[4] A. Hurwitz. Über die Komposition der quadratischen Formen. *Math. Ann.*, 88(1-2):1–25, (1922).

[5] P. Leopardi. Classifying bent functions by their Cayley graphs. In preparation.

[6] P. Leopardi. A generalized FFT for Clifford algebras. *Bulletin of the Belgian Mathematical Society – Simon Stevin*, 11(5):663–688, (2004).

[7] P. Leopardi. Constructions for Hadamard matrices, Clifford algebras, and their relation to amicability / anti-amicability graphs. *Australasian Journal of Combinatorics*, 58(2):214–248, (2014).

[8] P. C. Leopardi. Twin bent functions and Clifford algebras. In *Algebraic Design Theory and Hadamard Matrices*, 189–199. Springer, (2015).

[9] J. Radon. Lineare Scharen orthogonaler Matrizen. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 1(1):1–14, (1922).

[10] J. Williamson. Hadamard's determinant theorem and the sum of four squares. *Duke Math. J.*, 11:65–81, (1944).

[11] P. Y. Yiu. Strongly regular graphs and Hurwitz-Radon numbers. *Graphs and Combinatorics*, 6(1):61–69, (1990).